

# i春秋实验-肆虐的互联网泄密事件（撞库）

转载

[weixin\\_30627381](#) 于 2017-03-09 11:12:00 发布 283 收藏 2

文章标签: [python php](#)

原文链接: <http://www.cnblogs.com/solozhou/p/6524715.html>

版权

<http://www.ichunqiu.com/course/66>

实验环境:

操作机: windows xp

目标机: windows 2003

实验网站:

目标网址: [www.test.com](http://www.test.com)

whois: [www.whois.com](http://www.whois.com)

模拟泄漏库: [www.shegongku.com](http://www.shegongku.com)

实验文件:

dzuckey.py

实验工具:

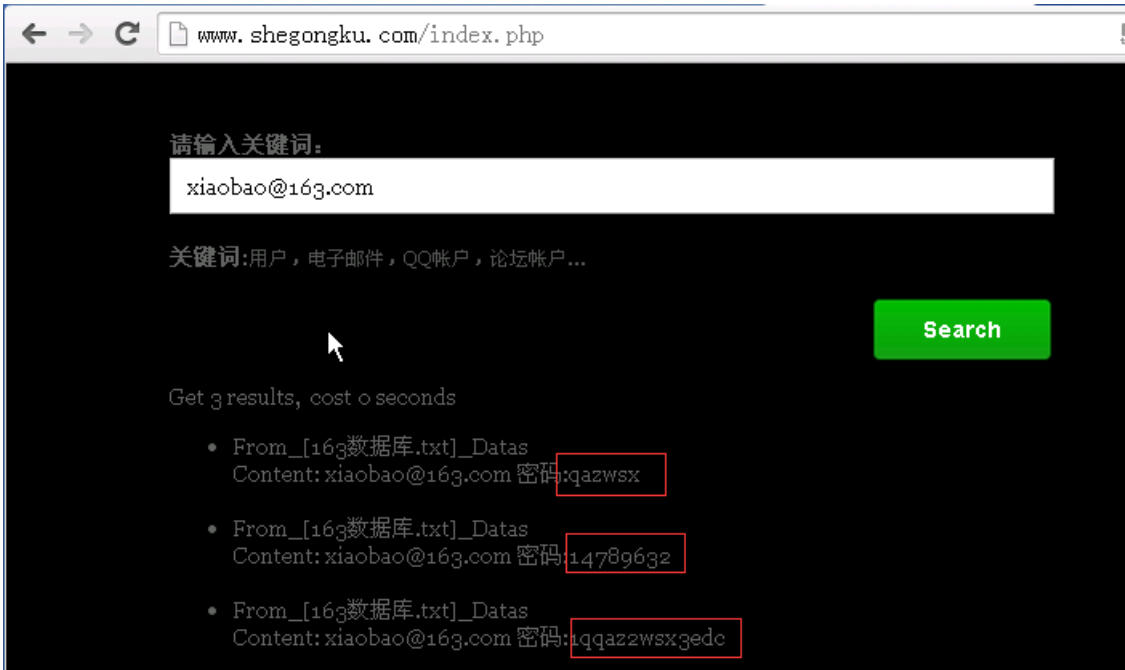
中国菜刀

实验步骤:

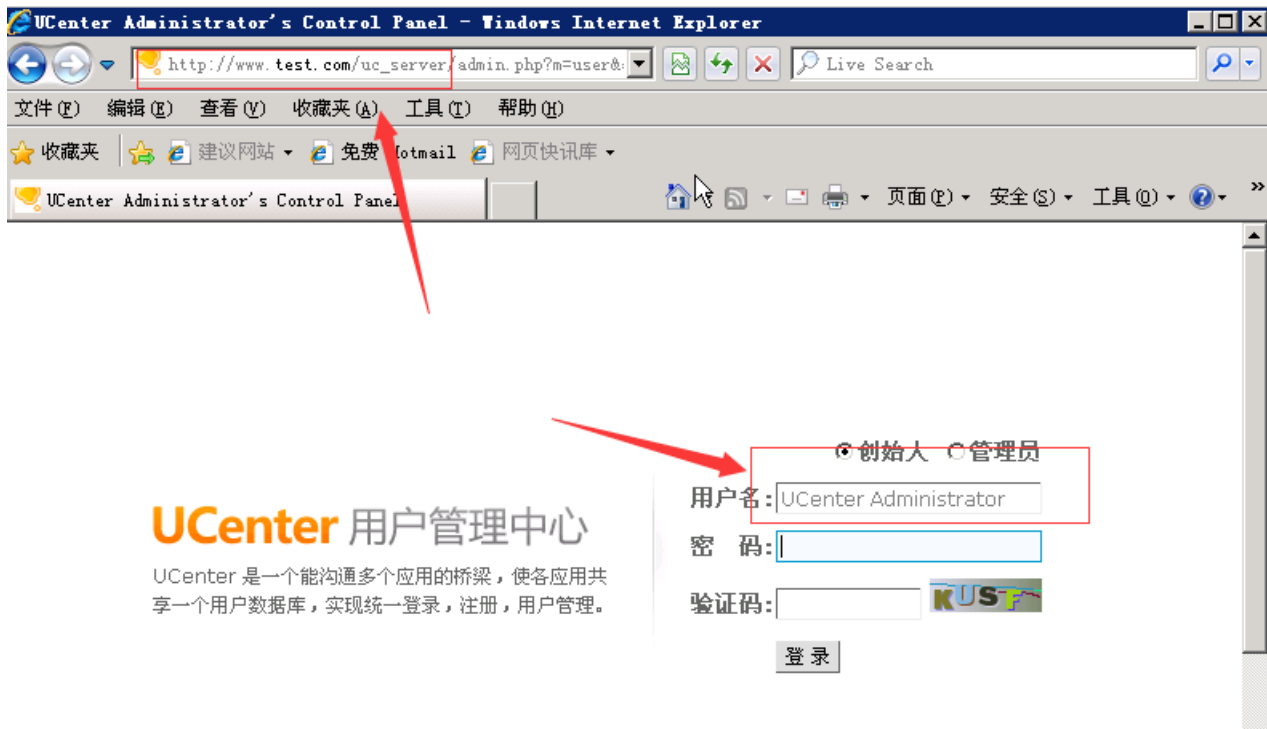
1、whois查询[www.test.com](http://www.test.com)网站信息，得到站长信息，如电话、qq号码、邮箱等，本实验得到邮箱 [xiaobao@163.com](mailto:xiaobao@163.com)

```
← → ↻ www.whois.com/?domain=www.test.com
Registrar URL: http://www.markmonitor.com
Creation Date: 2014-05-25T04:00:52-0700
Registrar Registration : 2015-05-25T04:05:17-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain_ " clientUpdateProhibited
Domain_ " clientTransferProhibited
Domain_ " clientDeleteProhibited
Registry Registrant ID:
Registrant Name: xiaobao
Registrant City: Beijing
Registrant State/Province: Beijing
Registrant Postal Code: 100085
Registrant Country: CN
Registrant Phone: +86.13881812525
Registrant Phone Ext:
Registrant Fax: +86.13881812525
Registrant Fax Ext:
Registrant Email: xiaobao@163.com
Registry xiaobao ID:
admin Name: xiaobao guo
admin City: Beijing
admin Fax Ext:
admin Email: xiaobao@163.com
Registry Tech ID:
```

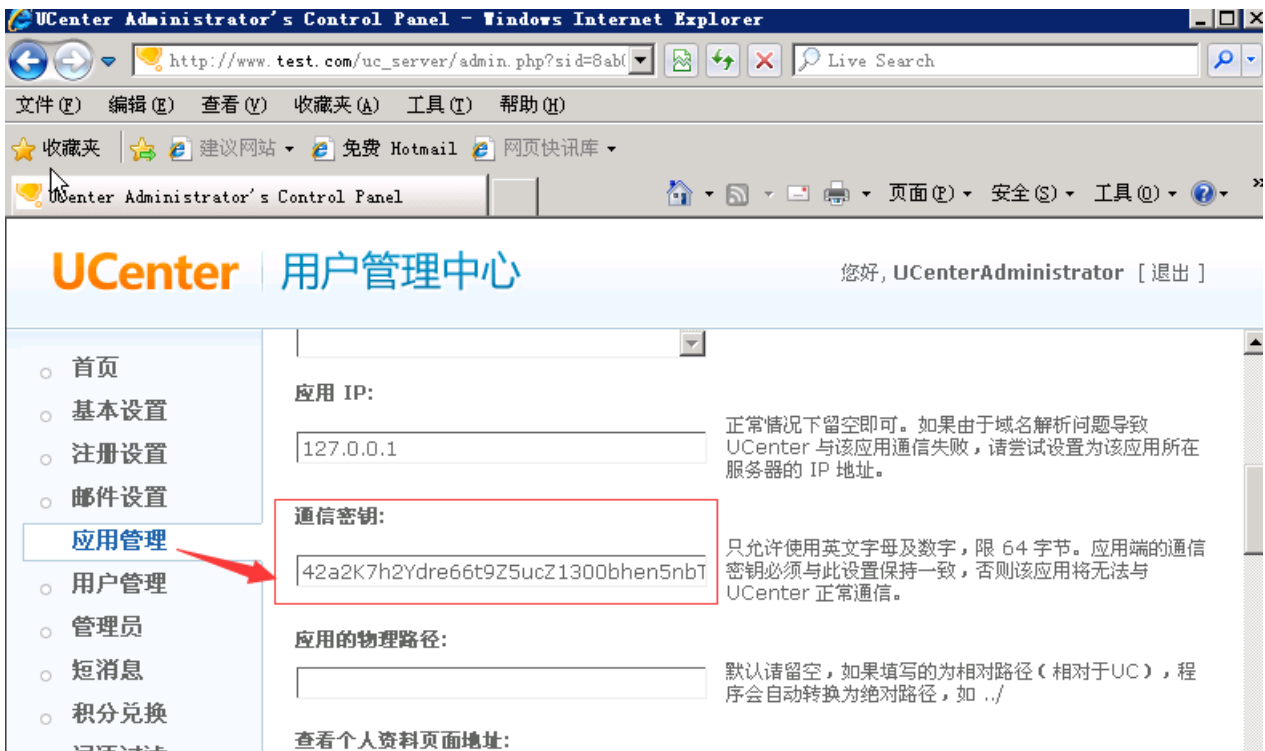
2、在社工科www.shengongku.com中输入站长邮箱得到3个密码qazwsx、14789632、1qqaz2wsx3edc



3、撞库测试，尝试利用密码组合撞库测试，网站后台/uc\_server，最终得到组合密码：qazwsx14789632



4、用后台UC\_KEY获取权限，后台-应用管理-通用密钥（UC\_KEY）获取UC\_KEY

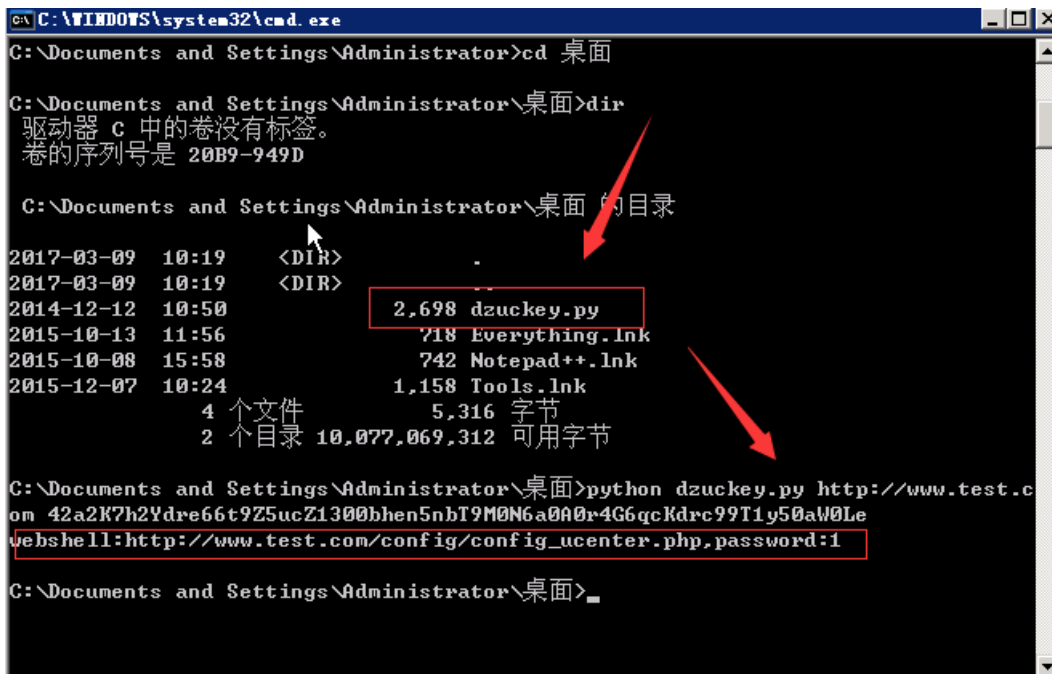


5、使用dzuckey.py脚本获取webshell:

```
cd:c:\ //切换至c盘根目录
```

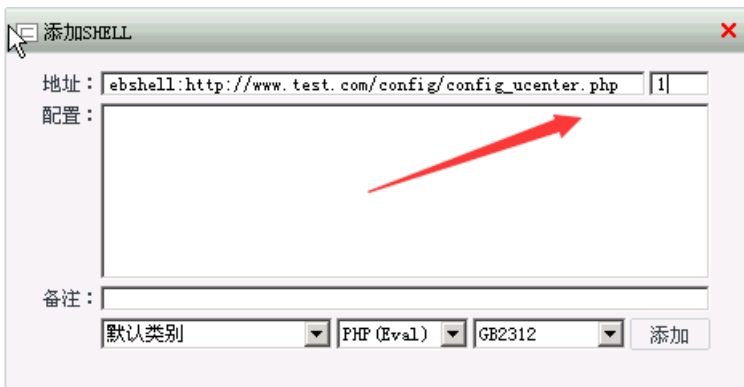
```
cd python27 //切换到python目录
```

```
python dzuckey.py www.test.com UC_KEY
```

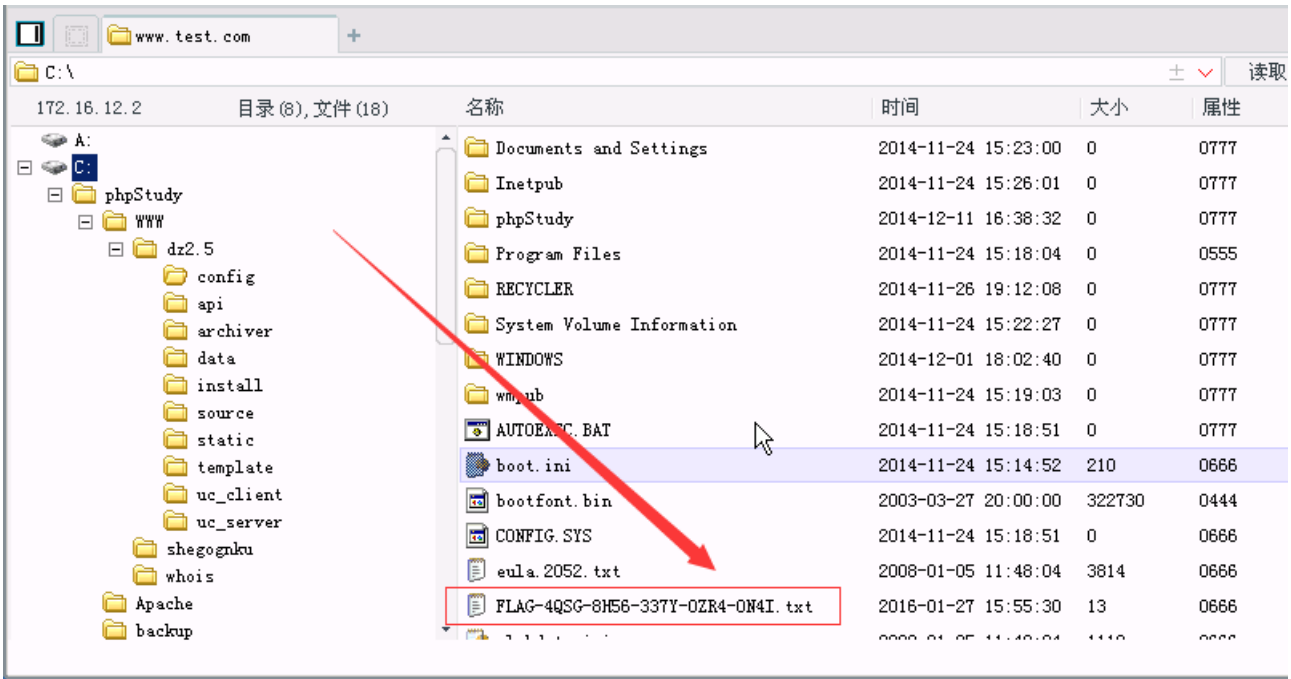


webshell:http://www/test.com/config/config\_ucenter.php 密码为1

6、使用中国菜刀连接webshell地址



## 7、查找flag



备注：**discuz**论坛有两个后台，一个是根目录下的/admin.php为网站管理后台、另一个是根目录下的/uc\_server/为网站用户管理中心，可以实现不用系统的统一登录功能。

撞库事件防护措施：

客户端防御：

- 1, 勿设置简单密码；
- 2, 密码长度不要太短；
- 3, 密码组合可适当复杂；
- 4, 使用手机、密保、令牌等硬件工具；
- 5, 多个网站多个密码，避免重复。

服务的防御：

- 1, 使用暗文密码；
- 2, 限制用户输入非常容易被破解的口令；
- 3, 妥善管理用户登录状态；

4, 口令探测防护;

5, 部署完善的信息安全系统。

转载于:<https://www.cnblogs.com/solozhou/p/6524715.html>